IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. :

U.S. National Serial No. :

Filed :

PCT International Application No. : PCT/FR00/00172

VERIFICATION OF A TRANSLATION

I, the below named translator, hereby declare that:

My name and post office address are as stated below;

That I am knowledgeable in the French language in which the below identified international application was filed, and that, to the best of my knowledge and belief, the English translation of the international application No. PCT/FR00/00172 is a true and complete translation of the above identified international application as filed.

I hereby declare that all the statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the patent application issued thereon.

Date: July 17, 2001

Full name of the translator : Roger Walter GRAY
For and on behalf of RWS Group plc

Post Office Address : Europa House, Marsham Way,
Gerrards Cross, Buckinghamshire,
England.

METHOD AND SYSTEM FOR CONTROLLING ACCESS TO A RESOURCE LIMITED TO CERTAIN TIMESLOTS, THE ACCESSING AND ACCESSED RESOURCES HAVING NO REAL-TIME CLOCK

The present invention relates to a method and a system for controlling access, by an accessing resource or electronic key, having no real-time clock, to an accessed resource or electronic lock, likewise having no real-time clock, this access being limited to certain timeslots.

It applies to the control of access to any accessed resource, the use of which one wishes to control, and access to which one wishes to limit to one or more determined timeslots, also known as predetermined validity slots, whether the relevant resource be a building, a computer system, or any other object, such as a mailbox or a bank safe.

The invention applies more particularly to the control of access to accessed resources which are not self-sufficient in terms of energy and/or are furnished with only a limited potential for checking a validity timeslot, in particular resources which are not furnished with any real-time clock.

The validity slot can be, either the actual period during which it is possible to access the resource, or any other parameter allowing a time limitation of an attack through fraudulent use of the accessing resource.

The main advantage of a logic means of access to a resource relative to a physical means of access generally lies in the possibility of precluding access to the resource other than within a relatively short predetermined timeslot.

Under these conditions, if the electronic key is lost, stolen, relinquished or duplicated, it will not allow its unlawful holder to access the resource outside of the predetermined timeslot. This presupposes however that the accessed resource is able to check that this timeslot is complied with. This generally implies that the accessed resource is furnished with a real-time clock.

Thus, the document FR-A-2 722 596 describes a system for controlling accesses which are limited to timeslots which are authorized and renewable by means of a portable memory medium. This system, based on cryptographic mechanisms, makes it possible to limit the period of validity of the rights of access to a short duration, in order to avoid unlawful use in the event of loss, theft, or illicit relinquishment or duplication.

However, the solution described relies on the highly constraining assumption that the accessed resource is self-sufficient in terms of energy, so as to maintain a real-time clock allowing it to check the validity of the timeslot in which the access attempt by the accessing resource takes place.

Access control methods and systems are also known in which the accessed resource comprises no real-time clock, but only a counter, reupdated after a successful access attempt of the accessing resource to the accessed resource.

However, in such methods and systems, the reupdating of the counter, in the accessed resource, is generally performed by the accessing resource, by means of a real-time clock with which the accessing resource is furnished.

A drawback of this solution is that it makes it necessary to ensure the energy self-sufficiency of the accessing resource, so that the latter can maintain its real-time clock permanently.

The aim of the present invention is to remedy the aforesaid drawbacks by allowing an accessed resource to check a validity slot associated with a right of access exhibited by an accessing resource whilst doing away with the need for the presence of a real-time clock, not only in the accessed resource, but also in the accessing resource.

With this aim, the present invention proposes a method of controlling access of at least one electronic key to at least one electronic lock, within a predetermined timeslot, according to which:

(a) prior to any attempted access of the electronic key to an electronic lock, a control time value, delivered by a real-time clock of an external validating entity, is stored in memory in the lock;

then, upon each attempted access of the electronic key to an electronic lock:

in the electronic key:

(b) a predetermined timeslot, previously stored in memory in the electronic key, is read;

(c) a trial time value, delivered by the real time clock of said external validating entity, is stored in memory in the key;

(d) the timeslot and the trial time value are transmitted from the electronic key to the electronic lock, and

in the electronic lock:

(e) it is checked that the trial time value transmitted is within the predetermined timeslot, and that it is posterior to the control time value stored in memory in the lock;

(f) if the checks performed in step (e) are satisfied, access is authorized and the control time value is updated on the basis of the trial time value transmitted;

(g) if the trial time value transmitted is outside the predetermined timeslot, or if it is anterior to the control time value stored in memory in the lock, access of this key to this lock is prohibited.

In an embodiment which affords enhanced security, the following additional steps are performed:

in the electronic key:

(b1) in step (b), an electronic signature of said timeslot, previously computed and stored in memory in the electronic key, is read in addition to the timeslot or instead of the timeslot;

(d1) in step (d), said electronic signature is transmitted from the electronic key to the electronic lock, on the one hand, in addition to or instead of the timeslot, and, on the other hand, of the trial time value, and

in the electronic lock:

(e1) before step (e), the signature transmitted is checked on the basis of a specific checking key;

(f1) in step (f), access is authorized and the control time value is updated, on the basis of the trial time value transmitted, only if the checks performed in steps (e1) and (e) are satisfied;

(g1) in step (g), access of the key to the lock is prohibited if the trial time value transmitted is outside the timeslot, or if it is anterior to the control time value stored in memory in the lock, or if the check performed in step (e1) is not satisfied.

As a variant, the order of execution of steps (e1) and (e) may be inverted.

The specific checking key used in step (e1) may be a public or secret key.

In another particular embodiment capable of affording enhanced security, the following additional steps are performed:

in the electronic key:

(c2) in step (c), in addition to the trial time value, an electronic signature of this trial time value is calculated and stored in memory;

(d2) in step (d1), the electronic signature of the trial time value is furthermore transmitted from the electronic key to the electronic lock, and

in the electronic lock:

(e2) before or after step (e), the signature of the trial value is checked, on the basis of a second public or secret specific checking key;

(f2) in step (f), access is authorized and the control time value is updated, only if the checks performed in steps (e), (e1) and (e2) are satisfied;

(g2) in step (g), access of the electronic key to the electronic lock is prohibited if one of the checks performed in steps (e), (e1) or (e2) is not satisfied.

The introduction of an electronic signature of the trial value is aimed at safeguarding the electronic key and the electronic lock against a type of fraud which would consist, in respect of a pirate furnished with an authentic timeslot value and an authentic trial time value, in modifying the trial time value in such a way that it becomes posterior to the control time value contained in the lock whilst remaining within the validity slot.

The aforesaid timeslot may comprise several disjoint timeslots.

In a particular embodiment, the timeslot is an interval comprising two bounds each expressed as a date in terms of day, month, year and a time in terms of hours, minutes, seconds.

The present invention also proposes a system for the electronic control of access, within a predetermined timeslot, comprising at least one electronic lock and at least one electronic key, wherein

the key comprises:

- a module for storing a trial time value, which module is read-accessible and write-accessible, and
- a module of communication for transmitting a predetermined timeslot and the trial time value to the lock, and wherein

the lock comprises:

- a module for storing a control time value, which module is read-accessible and write-accessible, and
- a module for comparing the trial time value with the predetermined timeslot and with the control time value stored in the module of storage of the lock.

In an embodiment which affords enhanced security, the communication module for transmitting a predetermined timeslot and the trial time value to the lock is accompanied by a module for transmitting an electronic signature of the timeslot and an electronic signature of the trial time value to the lock, and the lock furthermore comprises a module for checking the electronic signatures transmitted by the key.

In a particular embodiment, the module of storage comprises an electrically reprogrammable nonvolatile memory.

In a particular embodiment, the electronic key communicates with the electronic lock with the aid of a module of contactless transmission, by electromagnetic inductance.

This module of contactless transmission may comprise a first electromagnetic coil provided in the key and a second electromagnetic coil provided in the lock.

These two coils may be concentric.

The present invention also proposes an electronic key comprising at least one key computation logic unit, a module for transmitting/receiving key access control signals for implementing a method of controlling access between this electronic key and an electronic lock on the basis of lock access control signals produced by this electronic lock, this key being remarkable in that it furthermore comprises:

- a power signal generating module driven by the key computation unit; and
- a key transfer module for transferring key and lock access control signals and a power signal, the key transfer module comprising at least one winding interconnected with the power signal generating module and with the transmission/ reception module.

The present invention furthermore proposes an electronic lock comprising at least one lock computation logic unit and a module for transmitting/receiving lock access control signals for implementing a method of access control between this electronic lock and an electronic key on the basis of

key access control signals and of a power signal which are produced by this electronic key, this lock being remarkable in that it furthermore comprises:

- a lock transfer module of the key and lock access control signals and of the power signal, the lock transfer module comprising at least one winding interconnected with the module for transmitting/receiving lock access control signals; and
- a module for storing the electrical energy conveyed by the power signal, which is interconnected with the aforesaid winding.

Other characteristics and advantages of the present invention will become apparent on reading the detailed description which follows of particular embodiments, given by way of nonlimiting examples.

The description refers to the appended drawings in which:

figure 1 is a flow chart of the access control method of the present invention, in a first particular embodiment;

figure 2 is a flow chart of the access control method of the present invention, in a second particular embodiment;

- figure 3 is a flow chart of the access control method of the present invention in a third particular embodiment;

figure 4 diagrammatically represents the access control system of the present invention, in a first particular embodiment;

- figure 5 diagrammatically represents the access control system of the present invention, in a second particular embodiment;

- figure 6 diagrammatically represents the access control system of the present invention, in a third particular embodiment;

- figure 7 partly borrows figure 1a of French patent application filed under the number 98 10396; and

- figure 8 diagrammatically represents the module for contactless transmission allowing the electronic key to communicate with the electronic lock, in a particular embodiment.

Throughout what follows, consideration will be given to an electronic key used for an attempt to access an electronic lock. The electronic key and lock are furnished with a computation unit.

An external validating entity is fitted with a real-time clock. This real-time clock delivers a current time value VH expressed for example in the form day, month, year, hours, minutes, seconds.

One wishes to limit access of the key to the lock to a given timeslot PH, defined as the interval of time lying between two determined time values VH1 and VH2: PH = [VH1, VH2], or more broadly as a reunion of such intervals: PH = [VH1, VH2]$\cup$[VH3, VH4]$\cup$ ... $\cup$[VHn-1, VHn].

As indicated by figure 1, a first step 1001 of the method consists in storing in the electronic lock a time value VH_s, current time value delivered by the real-time clock of the aforesaid validating entity. By

convention, in everything that follows, this time value VH_s is called the "control time value VH_s".

Thereafter a situation is considered in which the electronic key attempts to access the electronic lock. This situation may pan out in various ways, depending on the form and the nature of the media containing the key and the lock. By way of nonlimiting example, if the key comprises a tubular part or one in the form of a flat shank, the access attempt is made by introducing the tubular part into a complementary tubular cavity of the lock, or into a complementary aperture, respectively.

A protocol for checking the right of access of this key to this lock is then implemented successively in the key and in the lock.

In the key, as indicated at 1002 in figure 1, a predetermined timeslot PH is read, this having previously been stored in memory in the electronic key.

As indicated at 1003, during the access attempt, a time value VH_c, current time value delivered by the real-time clock of the aforesaid validating entity is stored in memory in the key. By convention, in everything that follows, this time value VH_c is called the "trial time value VH_c".

Next, at 1004, the validity slot PH is transmitted together with the trial time value VH_c to the lock.

The following verification steps then take place in the lock.

At 1005 and 1006, the consistency between the trial time value VH_c transmitted and the predetermined timeslot PH is checked, on the one hand, as is the

consistency between VH_c and the control time value VH_s stored in memory in the lock, on the other hand.

For example, in the case of a timeslot reduced to an interval [VH1, VH2], one checks that VH_c is posterior to VH1 and anterior to VH2, and that VH_c is posterior to VH_s.

If one of the checks performed in steps 1005 and 1006 gives rise to a negative response, access of this key to this lock is prohibited.

If all these checks have been satisfied, access is authorized, and VH_s is updated by replacing it with, for example, the trial time value VH_c.

Another embodiment of the method of the invention, which affords enhanced security as compared with the previous embodiment, is described hereinbelow.

Consideration is given to an accessed resource which is not self-sufficient in terms of energy and/or is furnished with only a limited potential for checking a right of access.

The expression "right of access" is understood to mean the electronic signature of a validity slot. An electronic signature can be obtained with the aid of various cryptographic mechanisms, such as enciphering mechanisms or authentication mechanisms. It can for example be obtained with the aid of a secret key signature algorithm or of a public key signature algorithm.

When an "accessing resource", or "electronic key", presents a right of access to an "accessed resource", or "electronic lock", a right of access checking protocol is implemented. In this embodiment, this

protocol comprises, in addition to the checking of the validity slot, the checking of the electronic signature of this validity slot.

In this embodiment, the validity slot can either be the actual period during which it is possible to access the resource, or the period of validity of a signature key of the accessing resource allowing it to authenticate itself with regard to the accessed resource, or any other parameter allowing time limitation of an attack through fraudulent use of the accessing resource.

As indicated in figure 2, in this embodiment, a first step 2001 consists, just like in step 1001 in the previous embodiment, in storing in memory in the electronic lock a control time value VH_s, delivered by the validating entity.

In the case where the electronic signature S used is computed with the aid of a public key algorithm, of the RSA (Rivest Shamir Adleman) type for example, the public key K_p for checking the signature is stored in memory in the electronic lock. This public verification key K_p will have to be stored in such a way that it cannot be modified by an unauthorized entity. The key K_p will, as appropriate, be stored in a physically protected memory.

The electronic signature S can also be computed with the aid of a secret key algorithm, of the DES (Data Encryption Standard) type for example. In this case, unlike in the previous case, the checking key which is stored in memory in the lock in step 2001 is secret. Therefore, it will have to be stored within a physically protected memory, so that it can neither be read nor modified by an unauthorized entity.

Thereafter consideration is given to a situation in which the electronic key attempts to access the electronic lock. Just as in the previous embodiment, a protocol for checking the right of access of this key to this lock is implemented successively in the key and in the lock.

In the key, as indicated at 2002 in figure 2, an electronic signature S(PH) of the predetermined timeslot PH is read or established. This step takes place either in addition to or instead of step 1002 for reading the timeslot PH of the previous embodiment.

This electronic signature S(PH) may have been computed previously, for example by an outside entity for computing signatures, which is independent of the key.

In this case, during a loading step, for example by means of a validating terminal, the aforesaid validating entity transfers and stores the signature S(PH) in the key before this key is put into service.

As a variant, the key can itself establish the signature, if the private key required for this operation has been stored in the electronic key, together with the cryptographic signature algorithm, and if this key is furnished with the necessary computational resources.

As indicated at 2003, during the access attempt, the trial time value VH_c delivered by the validating entity is stored in memory in the key.

Then, at 2004, the electronic signature S(PH) of the validity slot is transmitted together with the trial time value VH_c to the lock. If, in step 2002, the timeslot PH has been read in addition to the signature

S(PH), this timeslot PH is also transmitted to the lock in step 2004.

The following checking steps then take place in the lock.

At 2005, the signature transmitted is checked. If the algorithm for computing signatures is a public key algorithm, step 2005 consists, in respect of the electronic lock, in applying the public key K_p, previously stored in memory in the lock, to the checking algorithm. A positive check of the signature makes it possible to ensure the authenticity of the validity slot [VH1,VH2], said slot being obtained either by reestablishing the message in the course of the signature checking step, or by simple reading if it has been transmitted unencrypted with the signature.

At 2006 and 2007, the consistency between the trial time value VH_c transmitted and the predetermined timeslot PH is checked, on the one hand, as is the consistency between VH_c and the control time value VH_s stored in memory in the lock, on the other hand.

For example, in the case of a timeslot reduced to an interval [VH1,VH2], one checks that VH_c is posterior to VH1 and anterior to VH2, and that VH_c is posterior to VH_s.

If one of the checks performed in steps 2005, 2006 and 2007 gives rise to a negative response, access of this key to this lock is prohibited.

If all these checks have been satisfied, access is authorized, and VH_s is updated by replacing it with, for example, the trial time value VH_c.

A third embodiment of the method of the invention, which is capable of affording enhanced security as compared with the previous embodiments, is described hereinbelow with the aid of figure 3.

Steps 3001 and 3002 illustrated in figure 3 are respectively identical to steps 2001 and 2002 of the previous embodiment and will not be described again.

As indicated at 3003 in figure 3, during an access attempt, the trial time value VH_c delivered by the validating entity is stored in memory in the key. Moreover, an electronic signature $S(VH_c)$ of the trial time value VH_c received originating from the validating entity is calculated and stored in memory in the key.

As a variant, this electronic signature $S(VH_c)$ can be calculated by a signatures computation unit independent of the key, for example contained in the validating entity.

In this case, upon delivery of the trial time value VH_c, the validating entity transfers and also stores in memory the signature $S(VH_c)$ in the key.

As a variant, the key can itself establish the signature of the trial value VH_c, if the private key necessary for this operation has been stored in memory in the electronic key, together with the cryptographic signature algorithm, and if this key is furnished with the necessary computational resources.

Next, the electronic signatures S(PH) of the validity slot PH and $S(VH_c)$ of the trial time value VH_c are transmitted to the lock, at 3004, together with the trial time value VH_c. If, at step 3002, the timeslot PH has been read in addition to the signature S(PH), this

timeslot PH is also transmitted to the lock in step 3004.

The following checking steps then take place in the lock.

At 3005, the signatures S(PH) and $S(VH_c)$ transmitted are checked, for example by means of one and the same checking algorithm. If the signatures computation algorithm is a public key algorithm, step 3005 consists, for the electronic lock, in applying the public key K_p, previously stored in memory in the lock, to the checking algorithm.

Positive verification of the signature S(PH) makes it possible to ensure the authenticity of the validity slot [VH1, VH2], this slot being obtained either by reestablishing the message during the signature checking step, or by simple reading if it has been transmitted unencrypted with the signature.

Positive verification of the signature $S(VH_c)$ makes it possible to ensure the authenticity of the trial time value VH_c.

The subsequent steps 3006 and 3007 are respectively identical to steps 2006 and 2007 of the previous embodiment and will not be described again.

If one of the checks performed in steps 3005, 3006 and 3007 gives rise to a negative response, access of this key to this lock is prohibited.

If all these checks have been satisfied, access is authorized, and VH_s is updated by replacing it with, for example, the trial time value VH_c, as in the previous embodiments.

A particular embodiment of the access control system in accordance with the present invention will now be described with the aid of figure 4.

The system comprises an electronic key 1 and an electronic lock 2.

The electronic key 1 comprises a memory 13, in which are stored the validity slot PH and a trial time value VH_c, such as that delivered by the external validating entity (not represented in figure 4) within the framework of the access control method described hereinabove.

The memory 13 is linked to a module 14 for communication of the key with the lock. The module 14 allows the key, during each access attempt, to transmit to a communication module 21 contained in the lock 2 the timeslot PH as well as the trial time value VH_c delivered by the validating entity, the values PH and VH_c being stored in the memory 13.

The module 21 for communication of the lock with the key is linked to a read-accessible and write-accessible memory 22, in which is stored a control time value VH_s, such as that delivered by the external validating entity within the framework of the access control method described hereinabove.

The control time value VH_s is reupdated, for example with the aid of the trial time value VH_c transmitted by the key 1, at each successful access attempt.

The memory 22 is for example an electrically reprogrammable memory of the EPROM or EEPROM type.

The electronic key 1 can, by way of nonlimiting example, be embodied in a form similar to that of an

assembly described in conjunction with figure 1a of French patent application filed as number 98 10396, reproduced as figure 7 of the present application. The content of the aforesaid application No. 98 10396 is incorporated by reference into the present description.

As shown by figure 7 of the present application, the electronic key 1 comprises a module 1_2 for transmitting/receiving key access control signals. This module 1_2 can comprise, advantageously, a module for transmitting key access control signals and a module for receiving lock access control signals. By convention, the key access control signals designate the access control signals transmitted by the key to the lock and the lock access control signals designate the access control signals transmitted by the lock to the key.

The electronic key 1 furthermore comprises, as indicated above, a computation unit, the so-called key computation logic unit 1_1. The key computation logic unit 1_1 makes it possible to control all the operations of the electronic key 1.

The electronic lock 2 also comprises, as indicated above, a computation unit, the so-called lock computation logic unit 2_1, and a module 2_2 for transmitting/receiving lock access control signals.

In a conventional manner, the lock computation logic unit 2_1 also makes it possible to control all the operations of the electronic lock 2.

Thus, under the respective control of the key and lock computation logic units 1_1 and 2_1, the modules for transmitting/receiving key and lock access control signals 1_2 and 2_2 allow the implementation of an access

control protocol between the electronic key 1 and the electronic lock 2.

The assembly represented in figure 7 of the present application furthermore comprises, at the level of the electronic key 1, a module 1_3 generating a power signal.

The power module 1_3 may be supplied from an external electrical energy source (not represented). As a variant, but not necessarily, the power module 1_3 can be supplied from an optional energy supply module 11, represented in figures 4, 5 and 6 of the present application, by way of nonlimiting example.

The power module 1_3 can be driven by the key computation logic unit 1_1.

Thus, the assembly of the functional modules for transmitting/receiving 1_2 key access control signals and power generator 1_3 is connected by a link to the key computation logic unit 1_1 and driven by the latter.

Furthermore, as shown by figure 7, the electronic key 1 comprises a first transfer circuit, the so-called key transfer circuit 1_4, allowing in particular the transferring of the key and lock access control signals and of the power signal produced by the power module 1_3. More precisely, the key transfer circuit 1_4 is linked, on the one hand, to the power module 1_3 and on the other hand, to the module for transmitting/ receiving key access control signals 1_2.

As shown by figure 7, the electronic lock 2 comprises a second transfer circuit, the so-called lock transfer circuit 2_4, allowing in particular the transferring of the key and lock access control signals and of the previously mentioned power signal.

Moreover, the electronic lock 2 also comprises a module 2_5 making it possible to ensure the storage and hence the recovery of the electrical energy conveyed by the power signal.

As shown in a nonlimiting manner by figure 7, the lock 2 can furthermore be fitted with a module 2_3 for recovering a clock signal.

The constituent functional modules of the electronic lock 2, that is to say, in the particular embodiment of figure 7, the module for transmitting/receiving the lock access control signals 2_2, the module for storing the electrical energy 2_5 and, as appropriate, the clock recovery module 2_3 are connected by way of a link to the lock computation logic unit 2_1.

The lock transfer circuit 2_4 is linked, on the one hand, to the module 2_2 for transmitting/receiving the lock access control signals and on the other hand, to the module 2_5 for storing the electrical energy as well as, as appropriate, to the clock recovery module 2_3.

In a nonlimiting advantageous manner, as shown by figure 7, the transfer circuit 1_4 of the key and the transfer circuit 2_4 of the lock can consist of the primary winding and the secondary winding of a transformer. Under such conditions, the primary winding, denoted L_1, and secondary winding, denoted L_2, are coupled from the electromagnetic point of view upon presentation of the electronic key and of the electronic lock, this presentation being effected so as to make an access attempt.

As shown by figure 4, the lock 2 furthermore comprises a comparison module 25, which receives the trial time value VH_c transmitted by the key 1, and compares it

with the predefined timeslot PH = [VH1,VH2] and with the control time value VH_s stored in the memory 22. The comparison module 25 tests whether $VH_c > VH1$ and $VH_c < VH2$, and whether $VH_c > VH_s$.

In a particular embodiment, as indicated above, the key 1 can furthermore comprise an energy supply module 11 for providing the lock 2 with the energy necessary for the checking operations performed by the comparison module 25, as well as with the energy required for the operation for reupdating the control time value VH_s stored in the memory 22 in the event of a successful access attempt.

As a variant, the key 1 comprises no energy supply module and the energy required for the checking and reupdating operations is provided by an external electrical energy source.

Described hereinbelow, with the aid of figure 5, is another embodiment of the access control system of the invention, comprising an electronic key 41 and an electronic lock 42, which affords enhanced security as compared with the embodiment of figure 4.

The elements of this system which are similar to those of the embodiment of figure 4 bear the same reference numerals, and will not be described again.

In this embodiment, the memory 13 of the key 41 contains not only the validity slot PH but also the electronic signature S(PH) of this validity slot.

The module 14 for communication of the key with the lock allows the key 41, during each access attempt, to transmit to the communication module 21 contained in the lock 42, not only the trial time value VH_c and the

timeslot PH which are stored in the memory 13, but also the electronic signature S(PH) stored in the memory 13.

The lock 42 comprises, in addition to the module 21 for communication with the key, to the memory 22 and to the comparison module 25, which were described previously, a signature checking module 24.

The module 24 is linked to the module 21 for communication of the lock with the key and to the comparison module 25. The module 24 receives the signature S(PH) of the validity slot and, in the case where the signatures computation algorithm used is a public key algorithm, checks the signature S(PH) received by means of the public key K_p.

As before, in a particular embodiment, the key 41 can furthermore comprise an energy supply module 11 for providing the lock 42 with the energy necessary for the checking operations performed by the signature checking module 24 and the comparison module 25, as well as with the energy required for the operation for reupdating the control time value VH_s stored in the memory 22 in the event of a successful access attempt.

As a variant, the key 41 comprises no energy supply module and the energy required for the checking and reupdating operations is provided by an external electrical energy source.

Described hereinbelow, with the aid of figure 6, is a third embodiment of the access control system of the invention, also comprising an electronic key 41 and an electronic lock 42, which is capable of affording enhanced security as compared with the previous embodiments.

The elements of this system which are similar to those of the embodiment of figure 5 bear the same reference numerals, and will not be described again.

In this embodiment, the memory 13 of the key 41 contains not only the validity slot PH and the electronic signature S(PH) of this validity slot but also the electronic signature $S(VH_c)$ of the trial time value.

The module 14 for communication of the key with the lock allows the key 41, during each access attempt, to transmit to the communication module 21 contained in the lock 42, not only the trial time value VH_c, the timeslot PH and the electronic signature S(PH), which are stored in the memory 13, but also the electronic signature $S(VH_c)$ stored in the memory 13.

The signature checking module 24 receives the signatures S(PH) of the validity slot and $S(VH_c)$ of the trial value, in the case where the signatures computational algorithm used is a public key algorithm, checks these signatures by means of the public key K_p.

As before, in a particular embodiment, the key 41 can furthermore comprise an energy supply module 11 for providing the lock 42 with the energy necessary for the checking operations performed by the signature checking module 24 and the comparison module 25, as well as with the energy required for the operation for reupdating the control time value VH_s stored in the memory 22 in the event of a successful access attempt.

As a variant, the key 41 comprises no energy supply module and the energy required for the checking and reupdating operations is provided by an external electrical energy source.

Figure 8 illustrates a particular hardware embodiment of the modules 14 and 21 for communication between the key and the lock, which is equally applicable to the embodiment of figure 4 as to the embodiments of figures 5 and 6.

The key 1 (or 41 in the case of the embodiments of figures 5 and 6) comprises a shank 30 made of ferromagnetic material, wrapped with copper windings 31 forming a first coil. This first coil is linked to the module 14 for communication of the key with the lock.

At each access attempt, the key 1 or 41 lodges in a tubular cavity 32 of slightly greater diameter than the diameter of the shank 30. The cavity 32 is also wrapped with copper windings 33 forming a second coil, linked to the module 21 for communication of the lock with the key. The two coils 31, 33 are then concentric, and the information is transmitted in binary coded form between the key and the lock 2, (or 42 in the case of the embodiment of figure 5) by electromagnetic induction).

The present invention finds an application particularly suited to access, by successive users, to resources which are made accessible to a given user only after having been freed by a previous user, and which, after this given user's access, no longer allows access to the previous user. The invention can thus be applied to resources such as hotel bedrooms or automatic lockers.

The security of the access control can be still further strengthened by adding other data to the signature and timeslot information transmitted by the key to the lock. For example, a serial number identifying the electronic key can be added. In this case, the lock may be fitted with a counting module, associated with this serial number. The start of the next timeslot in the course of which a key bearing this serial number will

be able to access the lock is stored in memory in this counting module.